

Docket No. 1095.1071/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Shuji OYAMA, et al.

Serial No.: To Be Assigned

Group Art Unit: To Be Assigned

Examiner: To Be Assigned

Filed: March 31, 1997

For: NETWORK TRANSACTION SYSTEM WITH AUTHENTICATION BASED ON
EXISTING BANK ACCOUNT

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, Applicant submits herewith a certified copy and an English translation thereof, of the following foreign application:

Japanese Patent Application No. 08-273153, filed October 16, 1996.

It is respectfully requested that Applicant be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY

Dated: March 31, 1997

By:

James D. Halsey, Jr.
Reg. No. 22,729

STAAS & HALSEY
700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1 9 9 6 年 1 0 月 1 6 日

出 願 番 号

Application Number:

平成 8 年特許願第 2 7 3 1 5 3 号

出 願 人

Applicant (s):

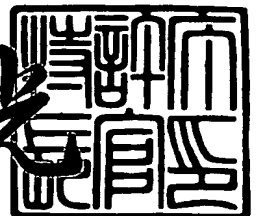
富士通株式会社

1 9 9 6 年 1 2 月 2 7 日

特 許 庁 長 官

Commissioner,
Patent Office

荒井 寿光



出証番号 出証特平 0 8 - 3 0 9 2 6 7 4

【書類名】 特許願

【整理番号】 9605459

【提出日】 平成 8年10月16日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/16

【発明の名称】 ネットワーク取引システム

【請求項の数】 13

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 尾山 修司

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 佐藤 昭

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

 【代表者】 関澤 義

【代理人】

 【識別番号】 100092152

 【弁理士】

 【氏名又は名称】 服部 毅巖

 【電話番号】 0426-45-6644

【手数料の表示】

 【予納台帳番号】 009874

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9207694

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク取引システム

【特許請求の範囲】

【請求項1】 複数の銀行の処理装置と前記銀行の少なくとも一つに既設の口座を有する顧客の処理装置とがネットワークを介して接続されるネットワーク取引システムにおいて、

顧客の既存口座に関する既存口座情報を取引を行おうとする仕向け銀行に送って新規口座開設の申込みを行う顧客処理手段と、

前記ネットワークを介して受けた前記既存口座情報を前記既存口座の存在する被仕向け銀行に銀行間ネットワークを利用して転送して本人確認の依頼をし、前記被仕向け銀行からの本人確認の依頼に対する応答を受けて新規に口座を開設する仕向け銀行処理手段と、

前記仕向け銀行から前記既存口座情報を添付した本人確認の依頼を受けて前記既存口座情報と登録口座情報とをチェックするとともに、チェックの結果を前記仕向け銀行へ返送する被仕向け銀行処理手段と、

を備えていることを特徴とするネットワーク取引システム。

【請求項2】 前記仕向け銀行処理手段は、前記既存口座情報が前記仕向け銀行に存在する口座である場合に、前記既存口座情報をチェックして口座開設の許可の判断を行うことを特徴とする請求項1記載のネットワーク取引システム。

【請求項3】 前記顧客処理手段は、新規に口座を開設するのに必要な口座開設情報をも送信するものであり、当該口座開設情報は、少なくとも顧客の氏名、住所、勤務先、仕向け銀行の銀行コード、新規申込口座に対する申込情報、新規申込口座の希望暗証を含むことを特徴とする請求項1記載のネットワーク取引システム。

【請求項4】 前記既存口座情報は、少なくとも顧客の口座が存在する銀行の銀行コード、顧客の口座番号、顧客の暗証を含むことを特徴とする請求項1記載のネットワーク取引システム。

【請求項5】 前記顧客処理手段は、顧客秘密鍵および顧客公開鍵を生成する秘密鍵／公開鍵生成手段と、新規に口座を開設するのに必要な口座開設情報を

前記顧客秘密鍵で暗号化してさらに仕向け銀行公開鍵で暗号化し、前記顧客公開鍵および被仕向け銀行の銀行コードを仕向け銀行公開鍵で暗号化し、さらに前記既存口座情報を前記顧客秘密鍵で暗号化したものをさらに被仕向け銀行公開鍵で暗号化して前記仕向け銀行に送るための口座開設申込電文を作成する暗号化手段と、前記仕向け銀行からの応答電文を前記顧客秘密鍵で復号化してさらに仕向け銀行公開鍵で復号化することにより新口座受付情報を得る復号化手段とを有することを特徴とする請求項1記載のネットワーク取引システム。

【請求項6】 前記仕向け銀行処理手段は、仕向け銀行秘密鍵および仕向け銀行公開鍵を生成する秘密鍵／公開鍵生成手段と、前記顧客処理手段から受信した口座開設申込電文の暗号化口座開設情報および暗号化した前記顧客公開鍵および被仕向け銀行の銀行コードを前記仕向け銀行秘密鍵で復号化して暗号化口座開設情報、前記顧客公開鍵および被仕向け銀行の銀行コードを得るとともに得られた前記顧客公開鍵で前記暗号化口座開設情報を復号化して前記口座開設情報を得、さらに、前記被仕向け銀行からの応答電文を被仕向け銀行公開鍵で復号して前記既存口座情報のチェックの結果を得る復号化手段と、前記仕向け銀行の銀行コード、顧客公開鍵および依頼番号を含む依頼情報を被仕向け銀行公開鍵で暗号化して前記顧客処理手段から受信された暗号化既存口座情報とともに前記被仕向け銀行への本人確認依頼電文を作成する暗号化手段とを有することを特徴とする請求項5記載のネットワーク取引システム。

【請求項7】 前記被仕向け銀行処理手段は、被仕向け銀行秘密鍵および被仕向け銀行公開鍵を生成する秘密鍵／公開鍵生成手段と、前記仕向け銀行からの本人確認依頼電文の暗号化依頼情報および暗号化既存口座情報を前記被仕向け銀行秘密鍵で復号化してさらに仕向け銀行公開鍵で復号化することにより仕向け銀行の銀行コード、顧客公開鍵および依頼番号を得るとともに復号化された前記暗号化既存口座情報を得られた前記顧客公開鍵で復号化して前記既存口座情報を得る復号化手段と、前記既存口座情報による口座の存在確認および暗証一致のチェックの結果、被仕向け銀行の銀行コードおよび前記依頼番号を前記被仕向け銀行秘密鍵で暗号化して仕向け銀行への応答電文を作成する暗号化手段とを有することを特徴とする請求項6記載のネットワーク取引システム。

【請求項 8】 複数の銀行処理装置と接続される、前記銀行の少なくとも一つに既設の口座を有する顧客の端末装置において、

新たに取引を行おうとする仕向け銀行に新規に口座を開設するのに必要な口座開設情報を送る際に、前記仕向け銀行が顧客の既存口座の存在する被仕向け銀行に対して本人確認を依頼するのに必要な顧客の既存口座に関する既存口座情報を添付する処理手段を備えていることを特徴とする端末装置。

【請求項 9】 前記処理手段は、前記口座開設情報を顧客秘密鍵で暗号化したものをさらに仕向け銀行公開鍵で暗号化した情報と、顧客公開鍵および被仕向け銀行の銀行コードを仕向け銀行公開鍵で暗号化した情報と、前記既存口座情報を前記顧客秘密鍵で暗号化したものをさらに被仕向け銀行公開鍵で暗号化した情報とを一緒にして、新規に口座を開設するための仕向け銀行への申込情報とすることを特徴とする請求項 8 記載の端末装置。

【請求項 10】 銀行間ネットワークによって接続されている複数の銀行の少なくとも一つに既設の口座を有する顧客に対してオープンネットワークを利用したあらゆる銀行とのサイバースペースバンキングを可能とするネットワーク取引における本人確認方式において、

前記顧客と新たに取引を行おうとする銀行は、新規に口座開設の申込みを受けるときに、口座開設に必要な口座開設情報と顧客の既存口座に関する既存口座情報とを受け取り、前記既存口座情報を既存口座が存在する銀行に送って前記顧客の本人確認を依頼し、前記本人確認の結果に基づいて口座開設の許可の判断をするように構成したことを特徴とするネットワーク取引における本人確認方式。

【請求項 11】 銀行間ネットワークによって接続されている複数の銀行の少なくとも一つに既設の口座を有する顧客に対してオープンネットワークを利用したあらゆる銀行とのサイバースペースバンキングを可能とするネットワーク取引における銀行の本人確認方法において、

顧客から、新規に口座を開設するのに必要な口座開設情報を顧客秘密鍵で暗号化したものをさらに仕向け銀行公開鍵で暗号化した第 1 の情報と、顧客公開鍵および顧客の口座が存在する被仕向け銀行の銀行コードを仕向け銀行公開鍵で暗号化した第 2 の情報と、顧客の既存口座に関する既存口座情報を顧客秘密鍵で暗号

化したものをさらに被仕向け銀行公開鍵で暗号化した第3の情報とを受け、

前記第2の情報を仕向け銀行秘密鍵で復号化して顧客公開鍵および被仕向け銀行の銀行コードを取得し、

前記第1の情報を仕向け銀行秘密鍵で復号化し、さらに前記顧客公開鍵で復号化して顧客の口座開設情報を取得し、

前記第3の情報と前記被仕向け銀行の銀行コード、顧客公開鍵および依頼情報を被仕向け銀行公開鍵で暗号化した第4の情報とを被仕向け銀行に送信して前記第3の情報に含まれる既存口座情報を基にした本人確認を前記被仕向け銀行に依頼し、

前記被仕向け銀行からの応答を受けて前記被仕向け銀行による本人確認の結果に基づいて口座開設の許可の判断をする、

ことを特徴とするネットワーク取引における銀行の本人確認方法。

【請求項12】 既存の口座を有する銀行とのオープンネットワークを利用したサイバースペースバンキングを可能とするネットワーク取引における口座保持銀行の本人確認方法において、

顧客から、新規に口座を開設するのに必要な口座開設情報および顧客の既存口座に関する既存口座情報を顧客秘密鍵で暗号化したものをさらに仕向け銀行公開鍵で暗号化した第1の情報と、顧客公開鍵を仕向け銀行公開鍵で暗号化した第2の情報とを受け、

前記第2の情報を仕向け銀行秘密鍵で復号化して顧客公開鍵を取得し、

前記第1の情報を仕向け銀行秘密鍵で復号化し、さらに前記顧客公開鍵で復号化して顧客の口座開設情報および既存口座情報を取得し、

前記既存口座情報を基にした本人確認を行い、

本人確認の結果に基づいて口座開設の許可の判断をする、

ことを特徴とするネットワーク取引における口座保持銀行の本人確認方法。

【請求項13】 既存の口座を有する銀行とのオープンネットワークを利用したサイバースペースバンキングを可能とするネットワーク取引における既存口座取引サービスでの本人確認方法において、

顧客から、既存口座に対するサービス内容を指示したサービス指示情報および

顧客の既存口座に関する既存口座情報を顧客秘密鍵で暗号化したものをさらに仕向け銀行公開鍵で暗号化した第1の情報と、顧客公開鍵を仕向け銀行公開鍵で暗号化した第2の情報とを受け、

前記第2の情報を仕向け銀行秘密鍵で復号化して顧客公開鍵を取得し、

前記第1の情報を仕向け銀行秘密鍵で復号化し、さらに前記顧客公開鍵で復号化してサービス指示情報および既存口座情報を取得し、

前記既存口座情報を基にした本人確認を行い、

本人確認の結果に基づいて既存口座に対するサービスを許可するかどうかの判断をする、

ことを特徴とするネットワーク取引における既存口座取引サービスでの本人確認方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はネットワーク取引システムに関し、特にオープンネットワークを利用した、新規口座開設、残高照会、取引明細照会、資金移動（振込、振替）などが可能なサイバースペースバンキング全般に適用することができ、さらには、クレジットカードなど業態内でお互いに通信することが可能なネットワークを持っている業態においても同様に適用することが可能なネットワーク取引システムに関する。

【0002】

従来より公衆網を使って自宅の端末機をあらかじめ決められた銀行のコンピュータと接続して顧客がその銀行に開設してある口座に対して取引照会や資金移動などのサービスを受けることが可能なホームバンキングは知られている。このようなホームバンキングでは、その銀行に既に口座を持っていることが前提であり、その口座の開設時には、その銀行では一般にその顧客が本人であることを証明するに足る何らかの証明書の提示が求められ、その証明書によって本人確認が行われている。

【0003】

【従来の技術】

インターネットなどのオープンネットワークを使って自分のパーソナルコンピュータ上に仮想の銀行の支店を開設し、実際に銀行に出向かなくても自宅の仮想銀行支店で銀行業務を遂行することができるようなサイバースペースバンキングが考えられている。このようなサイバースペースバンキングにおいても、通常の銀行と同様に本人確認が必要であるが、顧客が銀行に出向くことはないのでこの本人確認をどのようにして行うかが重要なポイントになっている。

【0004】

従来より提案されている本人確認方式としては、ネットワーク上に認証機関を設置しておき、その認証機関が発行する電子認証書を利用して本人確認を行うものとするものである。そのため、認証機関には、利用者があらかじめ郵便や本人出頭により登録の手続きをしておくことが必要であり、利用者の立場から見ると、電子認証書の取得が非常に煩わしいということがある。これでは、利用者の手間は現実の銀行に口座を開設するのとあまり変わらない。一方、銀行側の立場で見ると、認証機関への対応が煩わしいということがある。すなわち、認証機関自体の運営主体を誰にするのかということがあって、そのような認証機関を銀行が個別に作るのか、金融機関でまとめて一つ作るのかなど、現実にはまだ何も決まっていないのである。しかし、実際に実験的に行われているサイバースペースバンキングは、みな、認証機関の設置を前提とし、認証機関から発行された電子認証書で本人確認を行うようにしている。仮想銀行支店が自分のパーソナルコンピュータ上に移ってくると、従来のホームバンキングで受けられるサービスよりも広い範囲の業務取引が可能になる。

【0005】

【発明が解決しようとする課題】

しかし、サイバースペースバンキングを実験から普及に転換させようとするときには、利用者の電子認証書の取得の煩わしさおよび銀行の認証機関への対応の煩わしさが、大きな障害になり、新規の口座を簡単に作ることができなければ、普及も難しいという問題点があった。

【0006】

本発明はこのような点に鑑みてなされたものであり、認証機関を必要とすることなく利用者の本人確認が可能であり、銀行間ネットワークによって接続されたあらゆる銀行とのサイバースペースバンキングを可能にするネットワーク取引システムを提供することを目的とする。

【0007】

【課題を解決するための手段】

図1は上記目的を達成する本発明の原理図である。本発明のネットワーク取引システムは、複数の銀行1a, 1b, ...が銀行間ネットワーク2によって接続されており、かつサイバースペースバンキングを運営する銀行がオープンネットワーク3によって顧客4の端末機5に接続されているようなネットワーク環境において構築されるものであって、端末機5に設けられた顧客処理手段6と、口座の新約を行うたとえば銀行1aに設けられた仕向け銀行処理手段7と、顧客4の既存口座が存在するたとえば銀行1bに設けられた被仕向け銀行処理手段8とから構成される。

【0008】

顧客処理手段6は、顧客4が新規口座開設の申込みを行うとき、顧客4から新規に口座を開設するのに必要な口座開設情報および顧客の既存口座に関する既存口座情報の入力を受けて、これら口座開設情報および既存口座情報を銀行1aに送る。仕向け銀行処理手段7では、端末機5から口座開設情報および既存口座情報を受けると、まず、既存口座情報を顧客4の既存口座が存在する銀行1bに送り、被仕向け銀行処理手段8に対して顧客4の本人確認の依頼をする。この本人確認の依頼は銀行間ネットワーク2を利用して行われる。

【0009】

被仕向け銀行処理手段8は、送られた既存口座情報を銀行1bが保持している登録口座情報8aと照合して、既存口座情報から顧客4の既存口座が存在しかつ顧客4の口座であるかどうかをチェックする。そのチェックの結果は、銀行間ネットワーク2を通じて依頼元の銀行1aに返送される。銀行1aの仕向け銀行処理手段7では、被仕向け銀行処理手段8から本人確認依頼に対する応答を受け、チェックの結果を基に口座開設の許可の判断を行う。ここで、口座開設を許可す

ると判断された場合には、仕向け銀行処理手段 7 は新口座受付情報を端末機 5 に送って顧客 4 へ通知するとともに、新規口座開設の申込みの時に送られた口座開設情報を基に新規に口座 7 a を開設する。

【0010】

これにより、端末機 5 を使ってある銀行 1 a に新規に口座を開設しようとする場合に、顧客 4 は銀行間ネットワーク 2 によって結合されたいずれかの銀行 1 b に既存口座を持ってさえいれば、その銀行 1 b での認証を利用することにより、銀行 1 a では簡便に本人確認をすることができる。

【0011】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して説明するが、まず、本発明の概略について説明する。

【0012】

図 1 はネットワーク取引システムの原理構成を示す図である。本発明のネットワーク取引システムは、複数の銀行 1 a, 1 b, . . . が既存の銀行間ネットワーク 2 を利用して接続されており、かつサイバースペースバンキングを運営する銀行がオープンネットワーク 3 によって顧客 4 の端末機 5 に接続されているようなネットワーク環境において構築されるもので、端末機 5 に設けられた顧客処理手段 6 と、口座の新約を行うたとえば銀行 1 a に設けられた仕向け銀行処理手段 7 と、顧客 4 の既存口座が存在するたとえば銀行 1 b に設けられた被仕向け銀行処理手段 8 とから構成される。

【0013】

顧客処理手段 6 は、たとえばパーソナルコンピュータなどの端末機 5 内に実現される。ここで、顧客 4 が既存口座を保有していない銀行 1 a に新規口座開設の申込みを行うときには、顧客処理手段 6 は、顧客 4 から新規に口座を開設するのに必要な氏名、住所、新約口座の希望暗証などを含む口座開設情報および顧客 4 の既存口座が存在する銀行の銀行コード、口座番号、暗証などの既存口座情報の入力を受けて、これら口座開設情報および既存口座情報をオープンネットワーク 3 を通じて銀行 1 a に送る。銀行 1 a 内の仕向け銀行処理手段 7 では、端末機 5

から送られた口座開設情報および既存口座情報を受けると、まず、既存口座情報を顧客4の既存口座が存在する銀行1bに送り、被仕向け銀行処理手段8に対して顧客4の本人確認の依頼をする。この本人確認の依頼は銀行間ネットワーク2を利用して行われる。

【0014】

銀行1bの被仕向け銀行処理手段8では、送られた既存口座情報は銀行1bが保持している登録口座情報8aと照合され、その既存口座情報から顧客4の既存口座が存在していてかつ顧客4の口座であるかどうかをチェックする。そのチェックの結果は、銀行間ネットワーク2を通じて依頼元の銀行1aに返送される。銀行1aの仕向け銀行処理手段7では、被仕向け銀行処理手段8から本人確認依頼に対する応答を受けると、そのチェックの結果を基に顧客4の口座を開設していかどうかの判断を行う。ここで、口座を開設すると判断された場合には、仕向け銀行処理手段7は新規口座開設の申込みは受け付けられた旨の新口座受付情報を端末機5に送って顧客4へ通知する。また、仕向け銀行処理手段7は、新規口座開設の申込みの時に送られた口座開設情報を基にして銀行1aに新規の口座7aを開設する。

【0015】

これにより、端末機5を使ってある銀行1aに新規に口座を開設しようとする場合に、顧客4は銀行間ネットワーク2によって結合されたいずれかの銀行1bに既存口座を持ってさえいれば、口座新約を行う銀行1aは顧客4の既存口座が存在する銀行1bでの認証を利用することにより、特別な認証機関を必要とせずに簡便に本人確認をすることが可能になる。これは、銀行に既に口座を有しているということは、その口座を開設するときに既に本人確認が済んでいるということになるので、その銀行において本人確認をすることができれば、改めて本人を確認するための手続きは不要であることによる。また、当然ながら、口座新約を行う銀行1aに顧客4の既存口座が存在する場合は、その銀行1a内だけで、顧客4の本人確認をすることができる。この場合は、既存口座について、残高照会などのサービスだけを受けることもできる。

【0016】

次に、本発明の実施の形態を、インターネットなどのオープンネットワークを利用したサイバースペースバンキングに適用した場合を例にして説明する。口座を開設しようとする銀行には利用者本人の既設口座がない場合とある場合とがあるが、まず、口座を保有していない銀行に新規の口座を開設する場合から先に説明する。

【0017】

図2は本発明のネットワーク取引システムを適用したサイバースペースバンキングの構成例を示すブロック図である。顧客が利用する端末装置10はインターネットなどのオープンネットワーク20を介して口座の新約を行おうとする銀行の仕向け銀行装置30に接続されている。仕向け銀行装置30は、既存の銀行間ネットワーク40を利用することによって顧客の既存口座が存在する銀行の被仕向け銀行装置50に接続されている。

【0018】

端末装置10は、キーボードなどから入力された各種情報を処理する入力情報処理部11と、顧客の秘密鍵および公開鍵を生成する秘密鍵／公開鍵生成部12と、入力情報の暗号化および仕向け銀行装置30への電文伝送を行う暗号化部13と、仕向け銀行装置30からの応答電文の解読を行う復号化部14と、解読された情報の画面表示／プリンタ出力／保存を行う出力／保存処理部15と、端末装置10の動作履歴を保持するログ情報記憶部16とから構成される。仕向け銀行装置30は、仕向け銀行の秘密鍵および公開鍵を生成する秘密鍵／公開鍵生成部31と、端末装置10からの申込電文および被仕向け銀行装置50からの応答電文の解読を行う復号化部32と、確認依頼電文の暗号化および被仕向け銀行装置50への電文伝送と端末装置10への応答電文の暗号化および電文伝送とを行う暗号化部33と、解読された情報を基に口座新約の許可の判断を行う口座新約許可判断部34と、口座の情報を保持する口座情報記憶部35と、仕向け銀行装置30の動作履歴を保持するログ情報記憶部36とから構成される。被仕向け銀行装置50は、被仕向け銀行の秘密鍵および公開鍵を生成する秘密鍵／公開鍵生成部51と、仕向け銀行装置30からの確認依頼電文の解読を行う復号化部52と、仕向け銀行装置30への応答電文の暗号化を行う暗号化部53と、顧客の既

存口座のチェックを行う口座情報チェック部54と、口座の情報を保持する口座情報記憶部55と、被仕向け銀行装置50の動作履歴を保持するログ情報記憶部56とから構成される。

【0019】

ここで、端末装置10、仕向け銀行装置30および被仕向け銀行装置50において、新規口座開設に関する全体的な動作を図3を参照して以下に説明する。

図3は新規口座開設の処理手順を示すフローチャートである。まず、端末装置10において、入力情報処理部11が利用者から氏名、住所など、口座開設に必要な情報および既存口座の口座番号、口座暗証など、本人確認用の情報を取得し、暗号化部13はそれらの情報を暗号化して新規口座開設申込みの電文を作成し、その電文を仕向け銀行装置30へ伝送する（ステップS1）。仕向け銀行装置30では、端末装置10から新規口座開設申込みの電文を受け取ると、復号化部32がその電文を解読して口座開設に必要な情報および本人確認用の情報を取得し、暗号化部33がその本人確認用の情報から本人確認依頼電文を作成し、その電文を被仕向け銀行装置50へ伝送する（ステップS2）。被仕向け銀行装置50では、仕向け銀行装置30から本人確認依頼電文を受け取ると、復号化部52がその電文を解読して本人確認用の情報を取得し、口座情報チェック部54は本人確認用の情報と口座情報記憶部55に登録されている情報とを照合して一致しているかどうかをチェックし、暗号化部53はそのチェックの結果を暗号化して応答電文を作成し、その応答電文を仕向け銀行装置30へ伝送する（ステップS3）。仕向け銀行装置30では、その応答電文を復号化部32により解析して、被仕向け銀行装置50による本人確認のチェックの結果を取得し、口座新約許可判断部34がそのチェックの結果に基づいて口座の新約を許可するかしないかの判断をする（ステップS4）。次いで、その判断の結果が許可なのかどうか判定され（ステップS5）、許可である場合には、端末装置10から受信していた口座開設に必要な情報を基に口座が新規に作成され、その口座の情報は口座情報記憶部35に保持される（ステップS6）。口座が開設された場合または口座開設が許可されなかった場合の結果は、顧客からの照会に応じて、その結果は暗号化部33にて暗号化されて応答電文が作成され、その応答電文は端末装置10へ

新規口座開設申込みに対する受付結果として伝送される（ステップS7）。そして、端末装置10ではその応答電文は復号化部14にて解読され、得られた受付結果は出力／保持処理部15を通じて画面表示される。

【0020】

なお、これら一連の処理動作の中で、端末装置10、仕向け銀行装置30および被仕向け銀行装置50においてそれぞれ処理した履歴はそれぞれのログ情報記憶部16、36、56に記録保持される。

【0021】

次に、端末装置10、仕向け銀行装置30および被仕向け銀行装置50の間で伝送される情報およびその情報の暗号化について、図4を参照して以下に説明する。

【0022】

図4は暗号化情報の流れを示す説明図である。この例では、暗号化は、公開鍵を利用した暗号化方式であるRSA方式を使用するものとする。図4に示したように、端末装置10において、顧客Xの秘密鍵は p_x 、公開鍵は o_x で表すものとする。仕向け銀行装置30では、仕向け銀行Yの秘密鍵は p_y 、公開鍵は o_y で表し、被仕向け銀行装置50では、被仕向け銀行Zの秘密鍵は p_z 、公開鍵は o_z で表すものとする。

【0023】

まず、端末装置10において、仕向け銀行Yに新規に口座を開設するときに必要な情報として、

- a. 氏名、住所、勤務先、仕向け銀行Yの銀行コード、新規申込口座に対する申込情報、新規申込口座の申込暗証など、
- b. 顧客公開鍵 o_x 、被仕向け銀行Zの銀行コードなど、
- c. 被仕向け銀行Zの銀行コード、顧客Xの既存口座の口座番号、既存口座の口座暗証など、

があり、これらの情報は顧客Xによって与えられる。

【0024】

ここで、情報aは顧客秘密鍵 p_x で暗号化されてさらに仕向け銀行公開鍵 o_y

で暗号化される。この暗号化情報は、 F を暗号化関数とすると、 $F \circ y (F p x (a))$ で表すことができる。また、情報 b は仕向け銀行公開鍵 $o y$ で暗号化され、その暗号化情報は $F \circ y (b)$ で表される。情報 c は顧客秘密鍵 $p x$ で暗号化されてさらに被仕向け銀行公開鍵 $o z$ で暗号化され、その暗号化情報は $F \circ z (F p x (c))$ で表される。これらの暗号化情報は、平文の情報である

d. 電文フォーマットの規定コードなど、

を加えて、口座開設申込電文21が構成される。このため、この口座開設申込電文21は、

「 $F \circ y (F p x (a))$, $F \circ y (b)$, $F \circ z (F p x (c))$, d」

で表された形で仕向け銀行装置30に伝送される。

【0025】

仕向け銀行装置30では、受信した開設申込電文21の暗号化情報が復号化される。ここで、 Γ を復号化関数として、復号化処理を表すと、

$\Gamma p y (F \circ y (F p x (a))) \rightarrow F p x (a)$

$\Gamma p y (F \circ y (b)) \rightarrow b$

となる。さらに、 $F p x (a)$ を、復号化された情報 b に含まれている顧客公開鍵 $o x$ を使用して、復号化することにより、

$\Gamma o x (F p x (a)) \rightarrow a$

を得ることができる。なお、情報 c を暗号化した $F \circ z (F p x (c))$ は、最終的には被仕向け銀行公開鍵 $o z$ で暗号化されているので、それを仕向け銀行装置30において処理することはできず、そのままにされる。また、図示はしないが、ここで、新規口座開設申込みを受け付けたことおよびその受付番号を端末装置10へ返送する。

【0026】

次に、仕向け銀行装置30から被仕向け銀行装置50に伝送される確認依頼電文41は、暗号化情報 $F \circ z (F p x (c))$ と、

e. 仕向け銀行Yの銀行コード、顧客公開鍵 $o x$ 、依頼番号、

を仕向け銀行秘密鍵 $p y$ で暗号化してさらに被仕向け銀行公開鍵 $o z$ で暗号化した $F \circ z (F p y (e))$ と、平文の情報の

f. 電文フォーマットの規定コードなど、

とによって構成され、

「F o z (F p x (c)) , F o z (F p y (e)) , f」

で表される。

【0027】

被仕向け銀行装置50においては、受信した確認依頼電文41の暗号化情報が復号化される。すなわち、被仕向け銀行秘密鍵p zを用いて、

$\Gamma_{p z} (F o z (F p x (c))) \rightarrow F p x (c)$

$\Gamma_{p z} (F o z (F p y (e))) \rightarrow F p y (e)$

を得る。ここで、得られたF p y (e) を仕向け銀行公開鍵o yを用いて、

$\Gamma_{o y} (F p y (e)) \rightarrow e$

を得、この情報eに含まれている顧客公開鍵o xを用いることにより、

$\Gamma_{o x} (F p x (c)) \rightarrow c$

を得ることができる。

【0028】

この被仕向け銀行装置50では、情報cに含まれる顧客Xの既存口座の口座番号および口座暗証から、口座情報記憶部55に該当する口座番号が存在するかどうかの確認と、登録されている口座暗証と一致しているかどうかのチェックが行われることになる。

【0029】

そして、被仕向け銀行装置50は応答電文42の組み立てを行う。まず、

g. チェック結果、被仕向け銀行Zの銀行コード、依頼番号、

の情報を被仕向け銀行秘密鍵p zで暗号化し、これに

h. 電文フォーマットの規定コード、

が添付されて、「F p z (g) , h」の応答電文42が作られる。この応答電文42は仕向け銀行装置30に伝送される。

【0030】

その後、被仕向け銀行装置50は、履歴ログを取得してログ情報記憶部56に保存する。なお、口座暗証のチェックの際に、該当する口座はあるが、口座暗証

が一致しなかった場合には、事故防止のために、その口座に対する暗証エラーカウンタを+1する。

【0031】

次に、仕向け銀行装置30が受信した応答電文42の暗号化情報が復号化される。すなわち、被仕向け銀行公開鍵 o_z を用いることにより、

$$\Gamma o_z (F p_z (g)) \rightarrow g$$

を得ることができる。ここで、被仕向け銀行が正当かどうかのチェックが行われる。これは、仕向け銀行装置30があらかじめ保持している被仕向け銀行公開鍵 o_z を用いて復号化した情報 g の中にある被仕向け銀行Zの銀行コードが、あらかじめ保持している被仕向け銀行Zの銀行コードと一致するかをチェックすることによって行われる。

【0032】

次に、仕向け銀行装置30はチェック結果に基づく口座開設の判断を行う。ここでは、情報 g から、依頼番号に対するチェック結果がOKである場合のみ口座開設が許可されることになる。口座開設のときは、口座新設情報の保存が行われる。口座新設情報としては、住所、氏名、顧客公開鍵 o_x 、新規申込口座に対する暗証などであり、口座情報記憶部35に保持されることになる。そして、顧客の要求に従ってチェック結果に応じた端末装置10に対する応答電文22の組み立てが行われる。ここでは、

i. 仕向け銀行Yの銀行コード、受付結果、受付番号など、

j. 電文フォーマットの規定コードなど、

の情報が用意される。情報iは、仕向け銀行秘密鍵 p_y で暗号化され、さらに顧客公開鍵 o_x で暗号化される。したがって、応答電文22は、

$$「F o_x (F p_y (i)), j」$$

となり、端末装置10に伝送される。

【0033】

その後、仕向け銀行装置30は、履歴ログを取得してログ情報記憶部36に保存し、新規口座を開設する。

端末装置10では、受信した応答電文22の暗号化情報が復号化される。すな

わち、まず、顧客秘密鍵 p_x を用いることにより、

$$\Gamma_{p_x}(F_{o_x}(F_{p_y}(i))) \rightarrow F_{p_y}(i)$$

を得る。次に、仕向け銀行公開鍵 o_y を用いて、

$$\Gamma_{o_y}(F_{p_y}(i)) \rightarrow i$$

を得る。

【0034】

次いで、端末装置 10 は、仕向け銀行が正当かどうかのチェックを行う。これは、あらかじめ保持している仕向け銀行公開鍵 o_y を用いて復号化した情報 i の中にある仕向け銀行 Y の銀行コードが、あらかじめ保持している仕向け銀行 Y の銀行コードと一致するかをチェックすることによって行われる。ここで、仕向け銀行が正当なら、受付結果を画面表示したり、必要ならプリントを行い、かつ保存を行う。そして、端末装置 10 は履歴ログを取得し、ログ情報記憶部 16 に保存する。

【0035】

ここで、端末装置 10 において新規に口座を開設するときの口座申込の画面の一例を示す。

図 5 は新規口座開設の申込み画面の例を示す図である。この新規口座開設の申込み画面 60 は、端末装置 10 を新規に口座を開設したい仕向け銀行 Y の仕向け銀行装置 30 に接続したときに最初に表示されるサービスメニューの中から「新規口座開設」を選択し、さらに新規口座開設のサブメニューの中から「新規申込み」を選択することによって表示される。

【0036】

申込み画面 60 は、新規に口座を開設するときに必要な情報を入力する項目と、既存口座に関する情報を入力する項目とがある。ここでは、新規口座開設に必要な情報を入力する項目として、氏名および生年月日を入力する項目 61 と、住所および電話番号を入力する項目 62 と、勤務先および電話番号を入力する項目 63 と、申し込む口座の希望暗証番号を入力する項目 64 とを有している。これらの項目に入力された情報は、仕向け銀行装置 30 に送る際に、顧客秘密鍵および仕向け銀行公開鍵による暗号化の対象となる情報である。また、既存口座に関

する情報を入力する項目としては、既存口座の口座番号を入力する項目65および既存口座の暗証番号を入力する項目66を有している。口座番号は、銀行コードおよび支店コードを含めて入力するようにしている。これらの項目に入力された情報は、仕向け銀行装置30に送る際に、顧客秘密鍵および被仕向け銀行公開鍵による暗号化の対象となる情報である。申込み画面60は、さらに、申込みボタン67および取消しボタン68を有し、申込みボタン67は項目61～66への入力が済んだ後に、実際に新規口座開設の申込みを行うときに使用され、取消しボタン68は、この新規口座開設の申込みの処理をキャンセルするとき使用される。

【0037】

申込みボタン67によって新規口座開設の申込みを行うと、この申込み画面60にて入力された情報が仕向け銀行装置30に送られる。すると、仕向け銀行装置30は新規口座開設の申込みを受け付けた旨を受付番号とともに端末装置10に通知し、かつ、被仕向け銀行装置50に申し込み者の本人確認を依頼する。被仕向け銀行装置50による本人確認が取れて、仕向け銀行装置30が新規口座を開設すると判断すると、仕向け銀行装置30は新規口座開設の申込み時に受け付けた情報を基に口座を開設し、口座新設情報を保存する。ここで、端末装置10から受付番号による新規口座開設の状況照会がなされると、口座新設情報が端末装置10へ送られる。その際の画面の一例を以下に示す。

【0038】

図6は新規口座開設に対する状況照会の画面の例を示す図である。端末装置10において表示されるサービスメニューの「新規口座開設」のサブメニューには、「新規申込み」の他に「処理状況照会」が用意されており、その「処理状況照会」を選択することによって図示しない処理状況照会画面が表示される。そこで、新規口座開設申込みの後に通知された受付番号を入力し、照会の指示をすると、状況照会画面70が表示される。

【0039】

この状況照会画面70は、氏名の表示部71と、口座番号表示部72とを有しており、口座番号表示部72には、新規口座開設の申込みによって新規に開設さ

れた口座の番号が仕向け銀行装置30より受けて表示される。

【0040】

以上は口座を保有していない銀行に新規の口座を開設する場合について説明したが、次に、口座を保有している銀行に対して銀行取引を行う場合について説明する。この銀行取引には、新規に口座を開設する場合と、既存口座を利用したサービスの場合とがあり、まず、新規に口座を開設する場合について説明する。

【0041】

図7は本発明のネットワーク取引システムを適用したサイバースペースバンキングの別の構成例を示すブロック図である。顧客が利用する端末装置10はオープンネットワーク20によって既存口座を有しかつ口座の新約を行う銀行の仕向け銀行装置30に接続されている。

【0042】

端末装置10は、入力情報処理部11と、顧客の秘密鍵および公開鍵を生成する秘密鍵／公開鍵生成部12と、入力情報の暗号化および仕向け銀行装置30への電文伝送を行う暗号化部13と、仕向け銀行装置30からの応答電文の解読を行う復号化部14と、解読された情報の画面表示／プリンタ出力／保存を行う出力／保存処理部15と、端末装置10の動作履歴を保持するログ情報記憶部16とから構成される。仕向け銀行装置30は、仕向け銀行の秘密鍵および公開鍵を生成する秘密鍵／公開鍵生成部31と、端末装置10からの申込電文の解読を行う復号化部32と、端末装置10への応答電文の暗号化および電文伝送を行う暗号化部33と、口座新約の許可の判断を行う口座新約許可判断部34と、口座の情報を保持する口座情報記憶部35と、仕向け銀行装置30の動作履歴を保持するログ情報記憶部36と、申込み電文を基に顧客の既存口座のチェックを行う口座情報チェック部37と、既存口座の情報を保持する口座情報記憶部38とから構成される。

【0043】

まず、端末装置10において、顧客の既存口座を有する仕向け銀行に新規に口座を開設するときに、入力情報処理部11は以下の情報a1を顧客に対して要求する。

a 1. 氏名、住所、勤務先、仕向け銀行の銀行コード、新規申込口座に対する申込情報、新規申込口座の申込暗証、顧客の既存口座の口座番号、既存口座の口座暗証など。

【0044】

顧客によって入力された情報 a 1 は、次に、暗号化部 13 においてまず顧客秘密鍵 p x で暗号化され、さらに仕向け銀行公開鍵 o y で暗号化されて F o y (F p x (a 1)) となる。また、暗号化部 13 は、

b 1. 顧客公開鍵 o x

を仕向け銀行公開鍵 o y で暗号化して F o y (b 1) を生成する。そして、暗号化部 13 は、情報

d 1. 電文フォーマットの規定コードなど、

を加え、開設申込電文「F o y (F p x (a 1)), F o y (b 1), d 1」を組み立てて、仕向け銀行装置 30 に伝送する。

【0045】

仕向け銀行装置 30 では、受信した開設申込電文は復号化部 33 で復号化される。すなわち、復号化に仕向け銀行秘密鍵 p y を使用することによって、

$$\Gamma_{p y} (F o y (F p x (a 1))) \rightarrow F p x (a 1)$$

$$\Gamma_{p y} (F o y (b 1)) \rightarrow b 1$$

を得ることができる。さらに、情報 b 1 の顧客公開鍵 o x を使用して、F p x (a 1) を復号化することにより、

$$\Gamma_{o x} (F p x (a 1)) \rightarrow a 1$$

を得ることができる。

【0046】

復号化部 32 で得られた情報 a 1 の中の顧客の既存口座の口座番号および口座暗証が口座情報チェック部 37 に送られる。この口座情報チェック部 37 では、受けた口座番号から口座情報記憶部 38 を参照してそこに該当する口座番号が存在するかどうかの確認と、該当する口座番号が存在すれば、その口座番号に対して登録されている口座暗証と受けた口座暗証とが一致しているかどうかのチェックが行われる。そのチェックの結果は、口座新約許可判断部 34 に通知され、口

座を開設するか否かの判断が行われる。ここで、口座開設が許可されると、口座情報記憶部35に口座新設情報の保存が行われる。

【0047】

顧客からの処理状況照会があると、口座情報チェック部37によるチェック結果に応じた応答電文の組み立てが暗号化部33において行われる。すなわち、暗号化部33は、まず、

i1. 仕向け銀行の銀行コード、受付結果、受付番号など、
の情報を仕向け銀行秘密鍵 p_y で暗号化してさらに顧客公開鍵 o_x で暗号化し、
これに、

j1. 電文フォーマットの規定コードなど、
の情報を付加して、応答電文「 $F_{ox}(F_{py}(i1))$ 」, j1」を作成し、端末装置10に伝送する。

【0048】

端末装置10では、受信した応答電文は復号化部14で復号化される。まず、顧客秘密鍵 p_x を用いて、

$$\Gamma_{p_x}(F_{ox}(F_{py}(i1))) \rightarrow F_{py}(i1)$$

を得、さらに、仕向け銀行公開鍵 o_y を用いて、

$$\Gamma_{o_y}(F_{py}(i1)) \rightarrow i1$$

を得る。出力／保存処理部15は、新規口座開設申込に対する受付結果を画面表示などにより顧客に通知する。

【0049】

次に、口座を保有している銀行が既存口座を利用したサービスを行う場合について説明する。

既存口座を利用したサービスは、端末装置10の初期画面のサービスメニューの中から「ホームバンキング」を選択することによって、開始される。この場合、入力情報処理部11は以下の情報a2を顧客に要求する。

a2. 顧客の既存口座の口座番号、口座暗証、サービス依頼内容。

【0050】

次に、この情報a2は、暗号化部13においてまず顧客秘密鍵 p_x で暗号化さ

れ、さらに仕向け銀行公開鍵 o_y で暗号化されて $F o_y (F p_x (a_2))$ となる。また、暗号化部 13 は、

b2. 顧客公開鍵 o_x

を仕向け銀行公開鍵 o_y で暗号化して $F o_y (b_2)$ を生成する。そして、暗号化部 13 は、これらの暗号化情報に平文の情報

d2. 電文フォーマットの規定コードなど、

を加え、サービス申込電文「 $F o_y (F p_x (a_2))$ 」, $F o_y (b_2)$ 」, d2」を組み立てて、仕向け銀行装置 30 に伝送する。

【0051】

仕向け銀行装置 30 では、受信したサービス申込電文は復号化部 33 において復号化される。復号化部 33 は、まず、仕向け銀行秘密鍵 p_y を使用して、

$$\Gamma p_y (F o_y (F p_x (a_2))) \rightarrow F p_x (a_2)$$

$$\Gamma p_y (F o_y (b_2)) \rightarrow b_2$$

を得、さらに、情報 b_2 の顧客公開鍵 o_x を使用して、

$$\Gamma o_x (F p_x (a_2)) \rightarrow a_2$$

を得る。

【0052】

復号化部 32 で得られた情報 a_2 の中の顧客の既存口座の口座番号および口座暗証が口座情報チェック部 37 に送られる。この口座情報チェック部 37 では、受けた口座番号から口座情報記憶部 38 を参照してそこに該当する口座番号が存在するかどうかの確認と、該当する口座番号が存在すれば、その口座番号に対して登録されている口座暗証と受けた口座暗証とが一致しているかどうかのチェックが行われる。そのチェックの結果は、仕向け銀行装置 30 の中の図示しないサービス処理部に通知される。サービス処理部は、チェックの結果が「OK」ならば、情報 a_2 の中のサービス依頼内容を受けて、依頼内容に応じた処理を行う。依頼されるサービスの内容としては、残高照会、取引明細照会、資金移動などがある。

【0053】

そのサービスの依頼に対するサービス結果は、暗号化部 33 に送られ、応答電

文が作成される。

顧客からの処理状況照会があると、口座情報チェック部37によるチェック結果に応じた応答電文の組み立てが暗号化部33において行われる。すなわち、暗号化部33は、まず、

i 2. 仕向け銀行の銀行コード、サービス結果、受付番号など、
の情報を仕向け銀行秘密鍵 p_y で暗号化してさらに顧客公開鍵 o_x で暗号化し、
これに、

j 2. 電文フォーマットの規定コードなど、
の情報を付加して、応答電文「 $F o_x (F p_y (i 2))$ 」, j 2」を作成し、端末装置10に伝送する。

【0054】

端末装置10では、復号化部14において、受信した応答電文を顧客秘密鍵 p_x を用いて復号化することで、

$$\Gamma p_x (F o_x (F p_y (i 2))) \rightarrow F p_y (i 2)$$

を得、さらに、仕向け銀行公開鍵 o_y を用いて復号化することで、

$$\Gamma o_y (F p_y (i 1)) \rightarrow i 2$$

を得る。出力／保存処理部15は、復号化されたサービス結果を画面表示などにより顧客に通知する。

【0055】

【発明の効果】

以上説明したように本発明では、オープンネットワークを利用したサイバースペースバンキングにおいて、新規に口座を開設しようとする顧客の本人確認を、既に口座を有する銀行に行わせるように構成した。このため、銀行間ネットワークによって相互に接続されたいずれかの銀行に1個だけ口座が存在すれば、それはその銀行で既に本人確認は済んでいることになるので、その本人確認を既存の銀行間ネットワークを利用することによって他の銀行での本人確認をより簡便にすることができ、あらゆる銀行とのサイバースペースバンキングが可能になる。しかも、本人を確認するための認証機関への利用者の初期登録や、銀行による認証機関の維持管理を不要とし、銀行の認証機関への対応の煩わしさおよび利用者

の本人確認手続きの煩わしさをそれぞれ解消することができる。

【図面の簡単な説明】

【図 1】

ネットワーク取引システムの原理構成を示す図である。

【図 2】

本発明のネットワーク取引システムを適用したサイバースペースバンキングの構成例を示すブロック図である。

【図 3】

新規口座開設の処理手順を示すフローチャートである。

【図 4】

暗号化情報の流れを示す説明図である。

【図 5】

新規口座開設の申込み画面の例を示す図である。

【図 6】

新規口座開設に対する状況照会の画面の例を示す図である。

【図 7】

本発明のネットワーク取引システムを適用したサイバースペースバンキングの別の構成例を示すブロック図である。

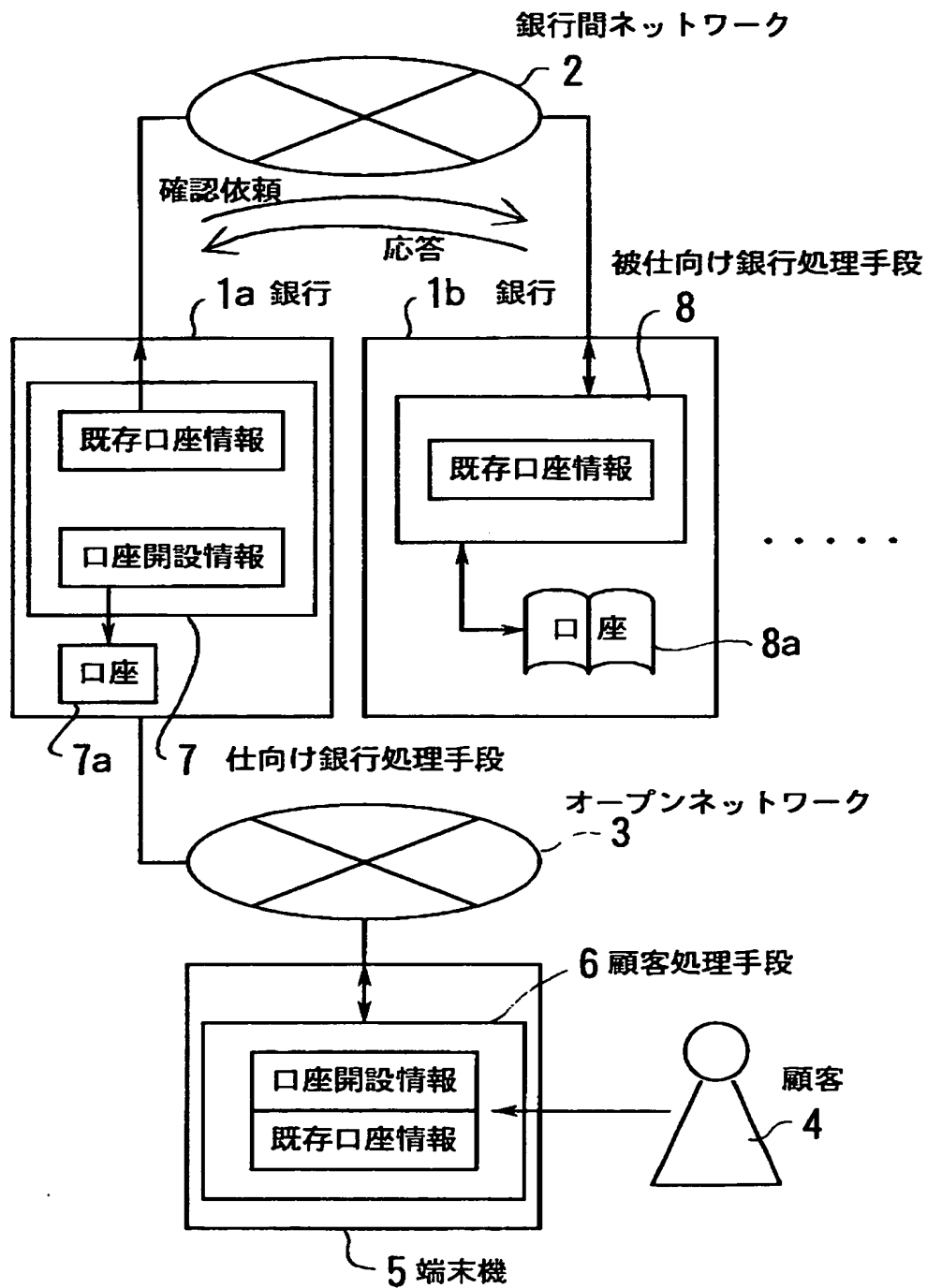
【符号の説明】

- 1 a, 1 b, . . . 銀行
- 2 銀行間ネットワーク
- 3 オープンネットワーク
- 4 顧客
- 5 端末機
- 6 顧客処理手段
- 7 仕向け銀行処理手段
- 8 被仕向け銀行処理手段
- 10 端末装置
- 20 オープンネットワーク

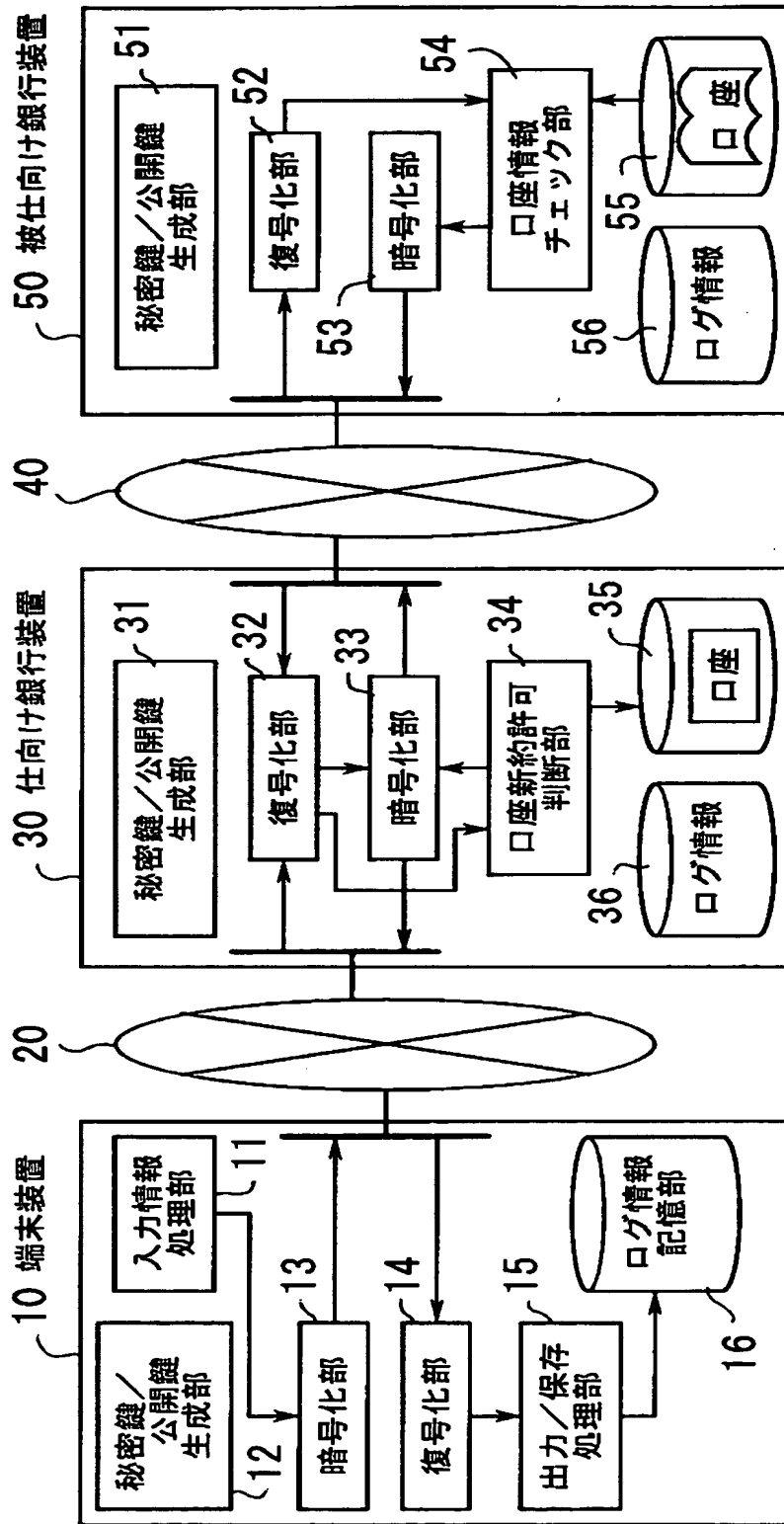
- 3 0 仕向け銀行装置
- 4 0 銀行間ネットワーク
- 5 0 被仕向け銀行装置
- 1 1 入力情報処理部
- 1 2 秘密鍵／公開鍵生成部
- 1 3 暗号化部
- 1 4 復号化部
- 1 5 出力／保存処理部
- 1 6 ログ情報記憶部
- 3 1 秘密鍵／公開鍵生成部
- 3 2 復号化部
- 3 3 暗号化部
- 3 4 口座新約許可判断部
- 3 5 口座情報記憶部
- 3 6 ログ情報記憶部
- 5 1 秘密鍵／公開鍵生成部
- 5 2 復号化部
- 5 3 暗号化部
- 5 4 口座情報チェック部
- 5 5 口座情報記憶部
- 5 6 ログ情報記憶部

【書類名】 図面

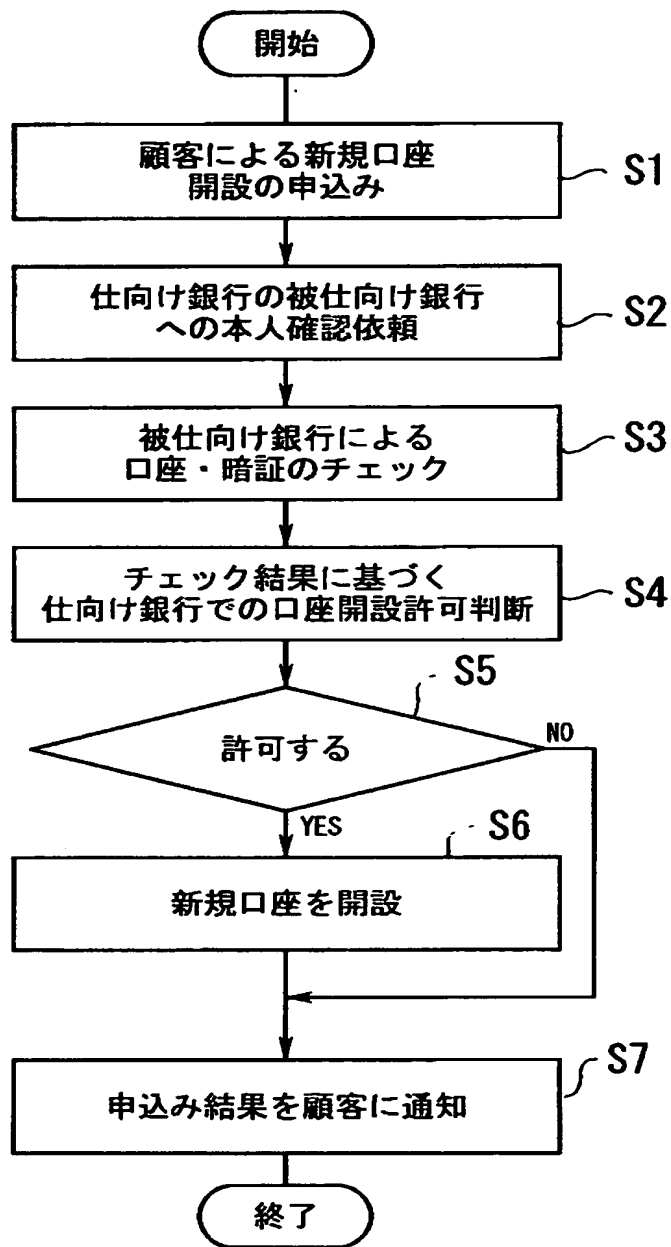
【図1】



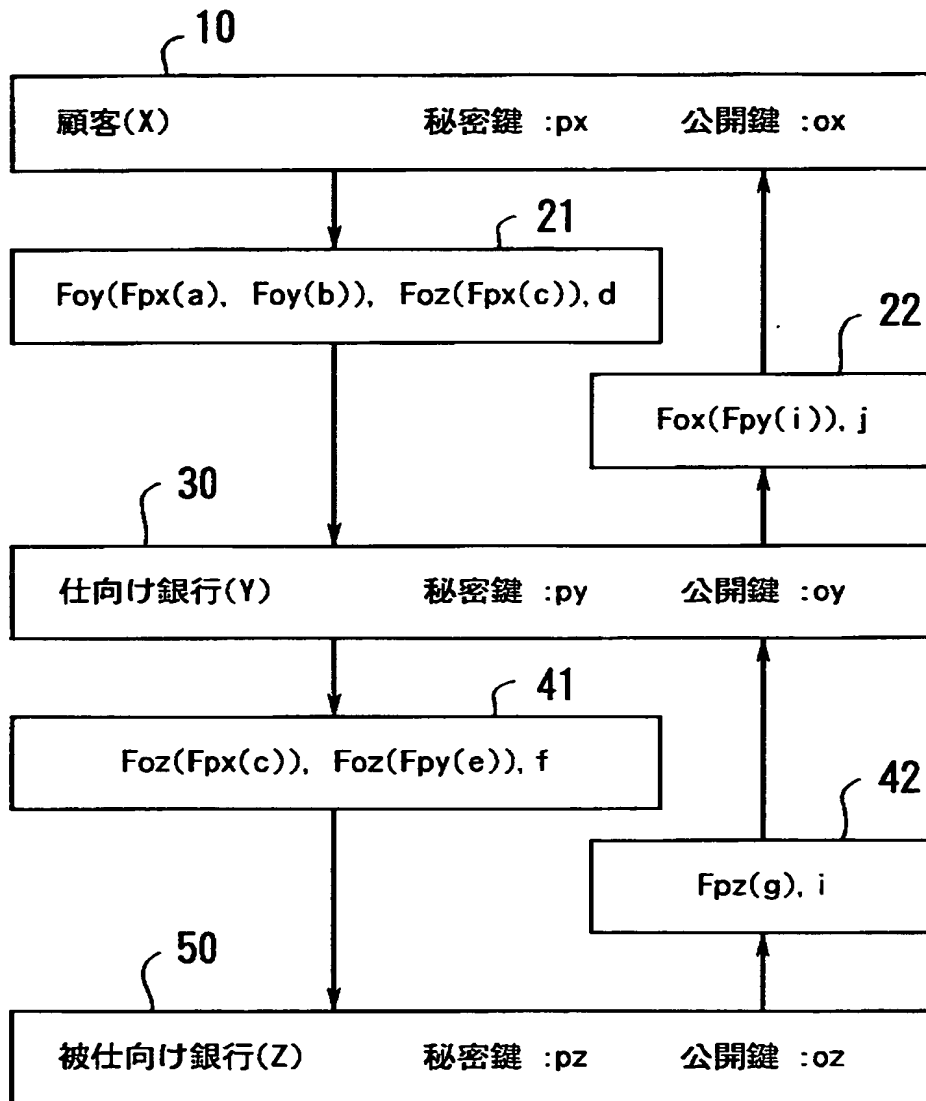
【図2】



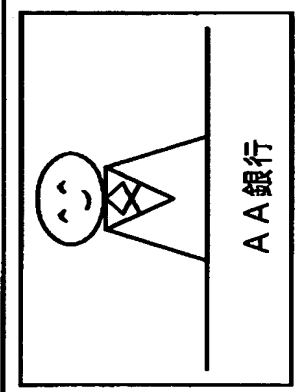
【図3】



【図4】



【図5】

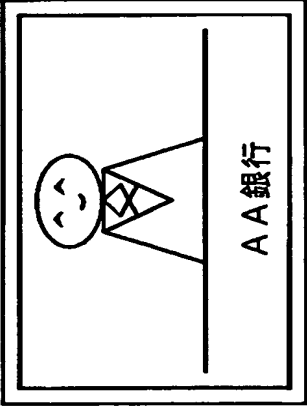



新規口座開設 申込み

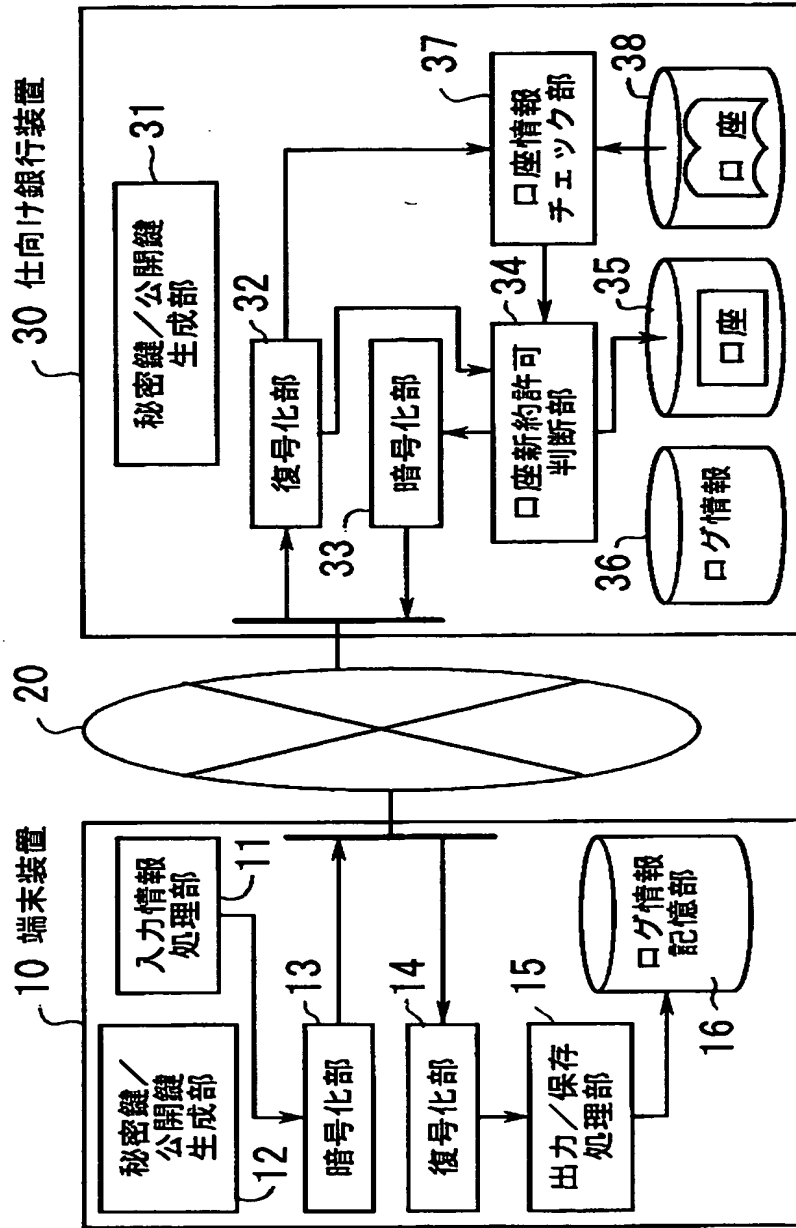
この度は、新規に口座を開設していただきありがとうございます。
口座の開設にあたって、下記の項目にご記入し、“申込み”ボタンを押してください。

- おなまえ フリガナ
- 生年月日 年 月 日 生 ☐ 男 ☐ 女
- おところ フリガナ
- 郵便番号 - 電話番号
- お勤め先 フリガナ 電話番号
- 申込暗証番号
- 既存口座の口座番号 - -
- 既存口座の暗証番号

【図6】

<div data-bbox="315 1142 620 1545">  </div> <div data-bbox="639 1121 695 1535"> <p>新規口座開設 状況照会</p> </div>	<p>この度は、新規に口座を開設していただきありがとうございます。</p> <p>71 <u>xxx xxx</u> 様</p> <p>の口座を開設させていただきました。</p> <p>72 <u>口座番号は 123-0123456</u> でございます。</p>	<p>通帳と銀行カードは郵便で別送しております。</p> <p>電子通帳と電子カードをご希望の場合は”受信”ボタンを押してください。</p>	<div data-bbox="1078 1478 1149 1577">  </div>
--	--	--	--

【図7】



【書類名】 要約書

【要約】

【課題】 ネットワーク取引システムに関し、オープンネットワークを利用したサイバースペースバンキングにて本人確認を簡便にすることを目的とする。

【解決手段】 顧客処理手段6では口座開設情報を顧客秘密鍵で暗号化したものを仕向け銀行公開鍵で暗号化し、顧客公開鍵および被仕向け銀行コードを仕向け銀行公開鍵で暗号化し、既存口座情報を顧客秘密鍵で暗号化したものを被仕向け銀行公開鍵で暗号化して仕向け銀行に送る。仕向け銀行処理手段7は仕向け銀行コードおよび顧客公開鍵を仕向け銀行秘密鍵で暗号化したものを被仕向け銀行公開鍵で暗号化して、暗号化されたままの既存口座情報と一緒に被仕向け銀行に送る。被仕向け銀行処理手段8では既存口座情報を解読して既存口座との比較をすることで本人確認を行い、その結果を仕向け銀行に通知する。仕向け銀行処理手段7は本人確認の結果を基に口座開設の許可の判断を行う。

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】
【識別番号】 000005223
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号
【氏名又は名称】 富士通株式会社
【代理人】 申請人
【識別番号】 100092152
【住所又は居所】 東京都八王子市東町9番8号 八王子東邦生命ビル
服部特許事務所
【氏名又は名称】 服部 毅巖

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社